



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.   | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------|------------------|
| 09/891,300  | 06/27/2001  | Sang-Woo Lee         | P-213               | 1619             |
| 34610   | 7590        | 10/18/2005           | EXAMINER            |                  |
| FLESHNER & KIM, LLP<br>P.O. BOX 221200<br>CHANTILLY, VA 20153 |             |                      | SHIFERAW, ELENI A   |                  |
|   |             |                      | ART UNIT            | PAPER NUMBER     |
|   |             |                      | 2136                |                  |
| DATE MAILED: 10/18/2005                                       |             |                      |                     |                  |

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/891,300

Applicant(s)

LEE, SANG-WOO

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 03 August 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☐ Claim(s) 1-7, 10-17 and 20-22 is/are pending in the application.
- 4a) Of the above claim(s) 8, 9, 18 and 19 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) \_\_\_\_\_ is/are rejected.
- 7) ☐ Claim(s) 1-7, 10-17 and 20-22 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 3, 2005 has been entered.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nagar et al. (Nagar, U.S. Patent No. 6,604,143 B1) in view of Coley et al. (Coley, U.S. Patent No. 6,061,798), and Schwartz et al. (Schwartz, Pub. No.: US 2002/0160790 A1).

As per claim 1, Nagar teaches a protective device for internal resource protection in a network, comprising:

a firewall (Nagar Fig. 2 No. 214) between an internal network (Nagar Fig. 2 No. 202; intranet) and an external network (Nagar Fig. 2 No. 204; internet), to selectively perform a disconnection function for an access request to the external network from the internal network (Nagar Col. 4 lines 62-col. 5 lines 6);

a FTP proxy (Nagar Fig. 2 No. 224) to perform an authentication function for an access request from the internal network to the external network (Nagar Col. 4 lines 62-col. 5 lines 48) and to record copies of data transmitted to the external network (Nagar Col. 5 lines 32-48); and

a file system to store data transmitted from the internal network to the external network according to the control of the FTP proxy (Nagar Col. 5 lines 32-48 and fig. 2 No. 242);

wherein the file system stores data according to a type of the data, and wherein the type of data is at least one of ASCII, EBCDIC, and Image (Nagar Col. 5 lines 32-48).

Nagar does not explicitly teach a database to store log information related to the transmission of data according to the control of the FTP proxy by an authenticated user;

Nagar's proxy determines access request using filter rule. Filter rule of Nagar does not explicitly teach registered ID/ IP address.

However **Coley** discloses a database to store transaction log that gathers information associated with any access request message seeking to connect to or inquire about network elements residing behind the firewall (Coley Col. 13 lines 24-36);

wherein the FTP proxy determines whether or not an ID transmitted from an internal user of the internal network is a registered ID (Coley col. 9 lines 35-48; checking the list of authorized and unauthorized/anonymous IP address on proxy database to control access);

wherein transmitting the data comprises:

checking an ID of the internal user if the received service command is a command request data transmission (Coley col. 9 lines 35-48, col. 6 lines 36-43, and col. 7 lines 37-65; proxy verifying list of authorized and non authorized IP address of requestors for file transfer);

if the user ID is "Anonymous," interrupting the transmission of the received service command to the external network (Coley col. 9 lines 35-62, and col. 10 lines 13-29; if requestors IP address is not on the list or the address is *unauthorized address(Anonymous)* then discard packet or deny access); and

if the user ID is a registered ID other than "Anonymous," transmitting the received service command to the external network and transmitting the data received from the internal user to the external network (Coley col. 9 lines 35-48 and col. 7 lines 37-65; if IP address is authorized and/or on the list then allowing file attaching/transmitting access).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Coley within the system of Nagar because it would store information like the identity of the machine from which the request originated, IP address which Internet port system did the request originate over, destination address, time of access, and identity of user to identify the identity of the user/hacker and enhance security (Coley Col. 13 lines 24-37).

Nagar and Coley fail to explicitly teach wherein access control is not performed if the ID transmitted from the internal user is "Anonymous," such that the internal user is permitted to connect to the server without access control.

**Schwartz** discloses wherein access control is not performed if the ID transmitted from the internal user is "Anonymous," such that the internal user is permitted to connect to the server

without access control (Schwartz par. 0036, and 0026; a proxy (link server 114) connecting anonymous mobile device IP address to a second mobile device of the second network without access control. Proxy account manager 312, that authenticates and verifies mobile devices and controls access to services, provides limited service to a anonymous mobile device/computer).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Schwartz within the combination system of Nagar and Coley because they are analogous in proxy authenticating an access request (abstract). One would have been motivated to incorporate the teachings of offering less access to anonymous IP address/user ID after connecting because it is very well known (Schwartz par. 0036) and it would restrict an authorized/anonymous user from sending confidential/unauthorized data/file to another network.

As per claim 2, Coley, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the device, further comprising a proxy monitor configured to display the log information outputted from the FTP proxy (Coley col. 6 lines 7-24, col. 9 lines 1-34, col. 13 lines 24-37).

As per claim 3, Coley, Nagar, and Schwartz teach all the subject matter as described above. In addition Nagar teaches the device, wherein a client connects to a FTP server of the external network through the FTP proxy (Nagar Col. 4 lines 56-67).

As per claim 4, Coley, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the device, wherein the log information comprises a file name and absolute path of the file data to be stored in the FTP server, and a file name and absolute path of the file data logged on the FTP proxy (Coley Col. 13 lines 24-35; Coley teaches a transaction log (information of user data transmitted) that gathers information associated with any access request message, therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to have log information that comprises a file name and absolute path of the file data to be stored in the FTP server, and a file name and absolute path of the file data logged on the FTP proxy because it would help to monitor the transmitted data file name, and path on the proxy).

4. Claims 5-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. (Coley, U.S. Patent No. 6,061,798) in view of Gupta et al. (Gupta, Pub. No. US 2001/0020242 A1), Nagar et al. (Nagar, U.S. Patent No. 6,604,143 B1), and Schwartz et al. (Schwartz, Pub. No.: US 2002/0160790 A1).

As per claim 5, Coley teaches a method for protecting internal resources in a network, comprising:

determining whether or not an access request is permitted by determining whether or not an ID transmitted from the internal user is a registered ID (Coley col. 9 lines 35-48, and Fig. 4B No. 428; checking the list of authorized and unauthorized/anonymous IP address on proxy database to control access);

receiving a service command (Coley Fig. 4B No. 436); and  
if the received service command is a command requesting data transmission,  
transmitting data from the internal user (Coley Col. 8 lines 29-44);

wherein transmitting the data comprises:

checking an ID of the internal user if the received service command is a command  
request data transmission (Coley col. 9 lines 35-48, col. 6 lines 36-43, and col. 7 lines 37-65;  
proxy verifying list of authorized and non authorized IP address of requestors for file transfer);

if the user ID is "Anonymous," interrupting the transmission of the received service  
command to the external network (Coley col. 9 lines 35-62, and col. 10 lines 13-29; if requestors  
IP address is not on the list or the address is *unauthorized address(Anonymous)* then discard  
packet or deny access); and

if the user ID is a registered ID other than "Anonymous," transmitting the received  
service command to the external network and transmitting the data received from the internal  
user to the external network (Coley col. 9 lines 35-48 and col. 7 lines 37-65; if IP address is  
authorized and/or on the list then allowing file attaching/transmitting access).

Coley does not explicitly teach if the received service command is a command  
designating a type of data, storing the designated type of data in a file system; and  
recording the transmission and reception of service;

However **Gupta** teaches storing different information in the proxy database when a  
request is transmitted from the client that reads on if the received service command is a  
command designating a type of data, storing the designated type of data in a file system (Gupta  
Page 4 col. 0057; it would have been obvious to one having ordinary skill in the art at the time of



the invention was made to store the designated type of data if the received service command is a command designating a type of data because it would help to identify the file data according to its data type);

recording the transmission and reception of service (Gupta Page 4 par. 0057); and  
wherein the file system stores data according to a type of the data, and wherein the type of data is at least one of ASCII, EBCDIC, and Image (Gupta par. 0057).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Gupta with in the system of Coley because it would allow the proxy to access the time that the user spends on particular website (Page 4 Par. 0057). Therefore it is obvious to have a file system to store data transmitted from the internal network to the external network according to the control of the FTP proxy because it would allow the operator to monitor which file has been transmitted by what user, and access requests from the internal network to the external network;

Coley and Gupta do not teach accessing an external network from an internal user of an internal network;

connecting to a server located in the external network if the access request is permitted;  
and

receiving a service command from the internal user.

However, **Nagar** teaches accessing an external network from an internal user of an internal network (Nagar Col. 4 lines 56-67);

connecting to a server located in the external network if the access request is permitted (Nagar Col. 4 lines 56-67; request from intranet user to internet server, Abstract; the request is then used to retrieve information from a server process); and

receiving a service command from the internal user (Nagar Col. 4 lines 56-67; proxy receives request command from intranet user to access the internet server).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Nagar within the system of Gupta and Coley and have a proxy server between an internal and an external network that performs authentication of an internal network users request to access an external network and transmission of data by an authenticated user, and to have database to store log files, and file system to store copies of data transmitted because it would authenticate a request from an internal network users to accessing an external server data.

Coley, Gupta, and Nagar fail to explicitly teach wherein access control is not performed if the ID transmitted from the internal user is "Anonymous," such that the internal user is permitted to connect to the server without access control.

**Schwartz** discloses wherein access control is not performed if the ID transmitted from the internal user is "Anonymous," such that the internal user is permitted to connect to the server without access control (Schwartz par. 0036, and 0026; a proxy (link server 114) connecting anonymous mobile device IP address to a second mobile device of the second network without access control. Proxy account manager 312, that authenticates and verifies mobile devices and controls access to services, provides limited service to a anonymous mobile device/computer).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Schwartz within the combination system of Coley, Gupta, and Nagar because they are analogous in proxy authenticating an access request (abstract). One would have been motivated to incorporate the teachings of offering less access to anonymous IP address/user ID after connecting because it is very well known (Schwartz par. 0036) and it would restrict an authorized/anonymous user from sending confidential/unauthorized data/file to another network.

As per claim 14, Coley teaches a method for protecting internal resources in a network, comprising:

giving a user of a local network in which a firewall is built a proper ID and host information (Coley Col. 7 lines 66-col. 8 lines 18, Fig. 4B; an external network user is given an ID and host information to required to enter id and host information therefore it would have been obvious to one having ordinary skill in the art to give a proper ID to an internal network user because it would help to authenticate an internal user to access an external network);

performing authentication (Coley Fig. 4B No. 428) and access control upon receiving a request for access (Coley Fig. 4B); and

storing log information in a database of a file system (Coley Col. 13 lines 24-37);

wherein transmitting the data comprises:

checking an ID of the internal user if the received service command is a command request data transmission (Coley col. 9 lines 35-48, col. 6 lines 36-43, and col. 7 lines 37-65; proxy verifying list of authorized and non authorized IP address of requestors for file transfer);

if the user ID is “Anonymous,” interrupting the transmission of the received service command to the external network (Coley col. 9 lines 35-62, and col. 10 lines 13-29; if requestors IP address is not on the list or the address is *unauthorized address(Anonymous)* then discard packet or deny access);

if the user ID is a registered ID other than “Anonymous,” transmitting the received service command to the external network and transmitting the data received from the internal user to the external network (Coley col. 9 lines 35-48 and col. 7 lines 37-65; if IP address is authorized and/or on the list then allowing file attaching/transmitting access); and

wherein the file system stores data according to a type of the data, and wherein the type of data is at least one of ASCII, EBCDIC, and Image (Coley Col. 13 lines 24-37);

Coley do not explicitly teach teaches transmitting file data transmitted from the internal user to the server and storing copies of the transmitted file data;

**Gupta** teaches transmitting file data transmitted from the internal user to the server and storing copies of the transmitted file data (Gupta Page 4 par. 0057);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Gupta with in the system of Coley because it would allow the proxy to access the time that the user spends on particular website (Page 4 Par. 0057). Therefore it is obvious to have a file system to store data transmitted from the internal network to the external network according to the control of the FTP proxy because it would allow the operator to monitor which file has been transmitted by what user, and access requests from the internal network to the external network;

Coley and Gupta do not explicitly teach teaches a request for access to an external network from the internal user;

connecting to a server of the external network if an access to the external network is permitted; and

receiving a service command from the internal user.

However **Nagar** teaches a request for access to an external network from the internal user (Nagar Col. 4 lines 56-67);

connecting to a server of the external network if an access to the external network is permitted (Nagar Col. 4 lines 56-col. 5 lines 48);

receiving a service command from the internal user (Nagar Col. 4 lines 56-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Nagar within the system of Gupta and Coley and have a proxy server between an internal and an external network that performs authentication of an internal network users request to access an external network and transmission of data by an authenticated user, and to have database to store log files, and file system to store copies of data transmitted because it would authenticate a request from an internal network users to accessing an external server data.

Coley, Gupta, and Nagar fail to explicitly teach wherein access control is not performed if the ID transmitted from the internal user is "Anonymous," such that the internal user is permitted to connect to the server without access control.

**Schwartz** discloses wherein access control is not performed if the ID transmitted from the internal user is "Anonymous," such that the internal user is permitted to connect to the server

without access control (Schwartz par. 0036, and 0026; a proxy (link server 114) connecting anonymous mobile device IP address to a second mobile device of the second network without access control. Proxy account manager 312, that authenticates and verifies mobile devices and controls access to services, provides limited service to a anonymous mobile device/computer).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Schwartz within the combination system of Coley, Gupta, and Nagar because they are analogous in proxy authenticating an access request (abstract). One would have been motivated to incorporate the teachings of offering less access to anonymous IP address/user ID after connecting because it is very well known (Schwartz par. 0036) and it would restrict an authorized/anonymous user from sending confidential/unauthorized data/file to another network.

As per claim 6, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method, wherein determining whether the access request is permitted comprises:

determining whether an ID transmitted from a user is a registered ID or not (Coley Fig. 4B No. 428; teaches determining whether an ID transmitted from the external user is a registered ID or not, it is obvious to determine whether an ID transmitted from the internal user is a registered ID or not); and

controlling access by determining whether a host that has transmitted the access request is a registered host or not, if the ID is a registered ID (Coley Fig. 4B No. 436; Coley discloses controlling access by determining whether a host that has transmitted the

access request is a registered host or not, if the ID of the external user is a registered ID, it would have been obvious to one ordinary skill in the art at the time the invention was made to control access by determining whether a host that has transmitted the access request is a registered host or not, if the ID of the internal user is a registered ID).

As per claim 7, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method, wherein controlling the access comprises:

reading host information corresponding to the registered ID using the registered ID (Coley Fig. 4B No. 440, Col. 8 lines 64-col. 9 lines 34);

determining whether the host information read from the database and the host that has transmitted the access request are identical or not (Coley Col. 9 lines 1-43);

permitting access if the two hosts are identical (Coley Col. 8 lines 64-col. 8 lines 34, Fig. 4B No. 440)

Nagar teaches reading host information corresponding to the registered ID from an internal database (Nagar Col. 4 lines 56-67);

permitting access to the external network (Nagar Col. 4 lines 56-67) The rationale for combining are the same as claim 1 above.

As per claim 10, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method, wherein recording the transmission and reception of services comprises:

receiving file data to be transmitted from the internal user to the external

network (Coley Col. 8 lines 29-67);

identifying the file data according to its data type to store the file data in the file system (Coley Col. 12 lines 65-col. 13 lines 15); and

recording log information on the transmission of file data in a database (Coley Col. 13 lines 29-49).

As per claim 11, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method, wherein the filed data can be identified by the user as a designated data type or can be identified as a default data type (Coley Col. 12 lines 65-col. 13 lines 15).

As per claim 12, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method, wherein the log information is recorded in the database (Coley Col. 13 lines 29-49)

when all data (user request) to be transmitted from the internal user to the external network is transmitted (Nagar Col. 4 lines 56-67). The rational for combining are the same as claim 1 above.

As per claim 13, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method, wherein the log information comprises a file name and absolute path of the file data to be stored in the FTP server, and a file name and absolute path of the file data logged on the FTP proxy (Coley Col. 13 lines 24-35; Coley teaches a



Art Unit: 2136

transaction log (information of user data transmitted) that gathers information associated with any access request message, therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to have log information that comprises a file name and absolute path of the file data to be stored in the FTP server, and a file name and absolute path of the file data logged on the FTP proxy because it would help to monitor the transmitted data file name, and path on the proxy).

As per claim 15, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method, wherein the authentication and access control comprises:

determining whether the ID transmitted is a registered ID (Coley Fig. 4B No. 428; teaches determining whether an ID transmitted from the external user is a registered ID, it is obvious to determine whether an ID transmitted from the internal user is a registered ID);

if the ID is registered, reading host information corresponding to the registered ID from the database (Coley Col. 8 lines 64-col. 9 lines 34, Fig. 4B No. 440);

determining whether the host information read from the database and the host who has transmitted the access request are identical (Coley Col. 9 lines 1-43);  
and

permitting access if the two hosts are identical (Coley Col. 8 lines 64-col. 8 lines 34, Fig. 4B No. 440).

Nagar teaches permitting access to the external network (Nagar Col. 4 lines 56-67) The rational for combining are the same as claim 1 above

As per claim 16, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method of claim 14, wherein storing copies of the transmitted file data and log information comprises:

receiving file data to be transmitted from the user to the external network (Coley Col. 8 lines 29-67);

identifying the file data according to a data type to thus store the file data in the file system (Coley Col. 12 lines 65-col. 13 lines 15); and

recording log information regarding the transmission of file data in a database (Coley Col. 13 lines 29-49).

As per claim 17, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method, wherein the log information comprises a user ID for performing file data transmission, a source IP address of the client being used by the internal user, a destination P address of the FTP server that receives the file data, a date and time of file data transmission, a file name and absolute path of the file data to be stored in the FTP server, and a file name and absolute path of the file data logged on the FTP proxy (Coley Col. 13 lines 19-37).

As per claim 20, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition

the device, further comprising a client (Nagar Fig. 2 No. 216), coupled to the firewall and to the FTP proxy (Nagar Fig. 2 No. 214), to request FTP service from the external network (Nagar Col. 4 lines 56-67) if the FTP proxy successfully authenticates the client (Coley Fig. 4B). The rationale for combining are the same as claim 1 above.

As per claim 21, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method further comprising outputting the login information in a form recognizable to a system operator (Coley Col. 13 lines 19-37, col. 9 lines 1-36).

As per claim 22, Coley, Gupta, Nagar, and Schwartz teach all the subject matter as described above. In addition Coley teaches the method, further comprising outputting the log information in a form recognizable by a system operator (Coley Col. 13 lines 19-37, col. 9 lines 1-36).

### ***Conclusion***

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. U.S. Patent 6,003,084 (Green et al.); proxy authenticating access requests by comparing the requestor's address received with requestor's address and the server's address stored on proxy access control list. If requestor's address is not registered/anonymous IP address, proxy closes/interrupts connection, and if requestor's address is registered, proxy generates a new connection.

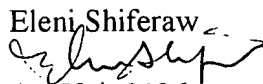
U.S. Patent 5,864,683 (Robert et al.); secure computer/proxy filtering data transferred


between the remote computer and the workstation. And assigning different access privileges to users.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw  
  
Art Unit 2136  
October 12, 2005

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100